Improper Access Control in Data Model Acceleration in Splunk Enterprise

Advisory ID: SVD-2026-0402

CVE ID: CVE-2026-20203 (https://www.cve.org/CVERecord?id=CVE-2026-20203)

Published: 2026-04-15

Last Update: 2026-04-15

CVSSv3.1 Score: 4.3, Medium

CVSSv3.1 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N (https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N)

CWE: CWE-284 (https://cwe.mitre.org/data/definitions/284.

Bug ID: VULN-25557

Description

In Splunk Enterprise versions below 10.2.2, 10.0.5, 9.4.10, and 9.3.11, and Splunk Cloud Platform versions below 10.4.2603.0, 10.3.2512.6, 10.2.2510.10, 10.1.2507.19, 10.0.2503.13, and 9.3.2411.127, a low-privileged user that does not hold the `admin` or `power` Splunk roles, has write permission on the app, and does not hold the high-privilege capability `accelerate_datamodel`, could turn on or off Data Model Acceleration due to improper access control.

For more information see Accelerate data models (https://help.splunk.com/en/splunk-enterprise/manage-knowledge-objects/knowledge-management-manual/10.2/use-data-summaries-to-accelerate-searches/accelerate-data-models) and Define roles on the Splunk platform with capabilities (https://help.splunk.com/en/splunk-enterprise/administer/manage-users-and-security/10.2/manage-splunk-platform-users-and-roles/define-roles-on-the-splunk-platform-with-capabilities).

Solution

Upgrade Splunk Enterprise to versions 10.2.2, 10.0.5, 9.4.10, 9.3.11, or higher.

Splunk is actively monitoring and patching Splunk Cloud Platform instances.

Product Status

Product	Base Version	Component	Affected Version	Fix Version
Splunk Enterprise	10.2	REST API	10.2.0 to 10.2.1	10.2.2
Splunk Enterprise	10.0	REST API	10.0.0 to 10.0.4	10.0.5
Splunk Enterprise	9.4	REST API	9.4.0 to 9.4.9	9.4.10
Splunk Enterprise	9.3	REST API	9.3.0 to 9.3.10	9.3.11
Splunk Cloud Platform	10.4.2603	REST API	Not Affected	Not Affected
Splunk Cloud Platform	10.3.2512	REST API	Below 10.3.2512.6	10.3.2512.6
Splunk Cloud Platform	10.2.2510	REST API	Below 10.2.2510.10	10.2.2510.10
Splunk Cloud Platform	10.1.2507	REST API	Below 10.1.2507.19	10.1.2507.19
Splunk Cloud Platform	10.0.2503	REST API	Below 10.0.2503.13	10.0.2503.13
Splunk Cloud Platform	9.3.2411	REST API	Below 9.3.2411.127	9.3.2411.127

Mitigations and Workarounds

None

Detections

None

Severity

Splunk rates this vulnerability a 4.3, Medium, with a CVSSv3.1 vector of CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N.

Acknowledgments

Mr Hack (try_to_hack) Santiago Lopez